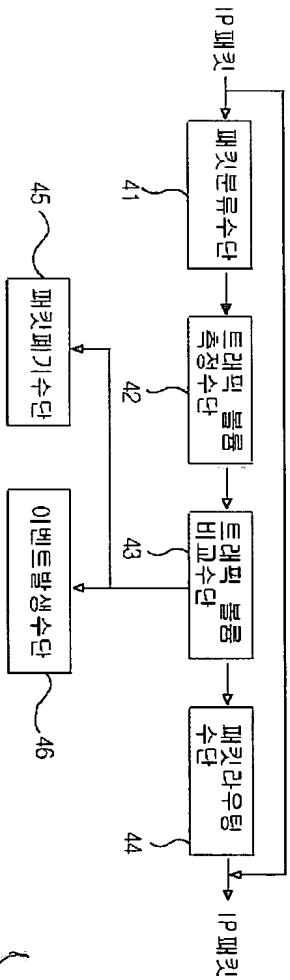
KOREAN PATENT ABSTRACTS(KR)

Document Code:A
(11) Publication No.1020030009887 (43) Publication.Date. 20030205
(21) Application No.1020010044551 (22) Application Date. 20010724
(51) IPC Code:
H04L 12/22

(71) Applicant:
KT CORPORATION
(72) Inventor:
KIM, SEONG HWAN
PARK, SEUNG EON
(30) Priority:

(54) Title of Invention
SYSTEM FOR INTERRUPTING DENIAL OF SERVICE ATTACK AND METHOD THEREFOR

Representative drawing



(57) Abstract:

PURPOSE: A system for interrupting DoS(Denial of Service) attack and a method therefor are provided to fundamentally interrupt the DoS attack by efficiently coping with the DoS attack through analysis traffic volume related to a destination address.

CONSTITUTION: A host connecting terminal analyzes the current bandwidth by analyzing a protocol of packets. The host connecting terminal compares a bandwidth assigned to the corresponding protocol with the current bandwidth. If the current bandwidth of the host connecting terminal is smaller than the assigned bandwidth, the corresponding packet is transmitted to a destination. If the current bandwidth of the host connecting terminal is

larger than the assigned bandwidth, the corresponding packet is abandoned.

if display of image is failed, press (F5)

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.		(11) 공개번호	특2003-0009887
H04L 12/22		(43) 공개일자	2003년02월05일
(21) 출원번호	10-2001-0044551		
(22) 출원일자	2001년07월24일		
---	---
(71) 출원인	주식회사 케이티 대한민국 463-815 경기 성남시 분당구 정자동 206
(72) 발명자	박승언 대한민국 305-390 대전광역시유성구전민동463-1
	김성환 대한민국 305-390 대전광역시유성구전민동463-1
(74) 대리인	전영일
(77) 심사청구	있음

(54) 출원명 서비스거부 공격 차단시스템 및 방법

요약

본 발명은 현재 인터넷 상에서 큰 문제로 대두되고 있는 서비스거부(DoS : Denial of Service) 공격 방지방법을 제공하기 위한 것이다.

본 발명에 따른 이러한 DoS 공격 차단시스템 및 방법은, 가입자 접속단에서 목적지 주소를 분석하고 목적지 주소 및 패킷의 종류별 트래픽 볼륨을 측정하여, 측정 트래픽 볼륨과 기준치를 비교하여 패킷을 전송하거나 폐기함으로써, DoS 공격을 차단한다. 본 발명의 방법을 가입자 접속단에 도입하면 DoS 공격을 근원적으로 효율적으로 차단할 수 있다. 즉, 망사업자 입장에서 보면 공격 트래픽을 출발지에서 차단함으로써 폭주로 인한 망 자원 고갈 및 성능저하 같은 피해를 막을 수 있고, 호스트 입장에서도 집중적인 트래픽 공격을 출발지에서 차단해 줌으로써 실제적으로 DoS 공격을 피할 수 있게 되는 효과가 있다.

대표도

도3

색인어

서비스거부 공격, DoS, 목적지주소, 트래픽 볼륨, 패킷

명세서

도면의 간단한 설명

도 1은 일반적인 서비스거부(DoS) 공격이 발생하는 서비스망을 도시한 도면,

도 2는 종래의 가입자 접속단에서의 출발지 주소 분석을 통한 DoS 공격 차단방법을 도시한 동작 흐름도,

도 3은 종래의 호스트 접속단에서의 트래픽 볼륨 분석을 통한 DoS 공격 차단방법을 도시한 동작 흐름도,

도 4는 본 발명에 따른 가입자 접속단에서의 DoS 공격 차단시스템을 도시한 구성 블록도,

도 5는 본 발명에 따른 가입자 접속단에서의 목적지 주소 분석을 통한 DoS 공격 차단방법을 도시한 동작 흐름도이다.

※ 도면의 주요 부분에 대한 부호의 설명 ※

41 : 패킷 분류수단∘∘∘∘42 : 트래픽 볼륨 측정수단

43 : 트래픽 볼륨 비교수단∘∘∘44 : 패킷 라우팅수단

45 : 패킷 폐기수단∘∘∘∘46 : 이벤트 발생수단

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 인터넷 상에서의 서비스거부(DoS : Denial of Service) 공격 방지시스템 및 방법에 관한 것으로서, 보다 상세하게 설명하면 공격의 근원이 되는 가입자 접속단에서 목적지(Destination) 주소를 분석하고 차단조치를 취함으로써 DoS 공격을 원천적으로 방지하는 시스템 및 방법에 관한 것이다.

서비스거부(DoS) 공격이란, 외부 공격자가 특정 컴퓨터 시스템의 정상적인 운영을 방해하여 그 컴퓨터 시스템이 사용자에 대한 서비스의 제공을 거부하도록 하는 것을 말한다. 서비스거부 공격방법의 일례로 한 사용자가 특정 시스템의 리소스를 독점하거나 파괴함으로써, 다른 사용자들이 그 시스템의 서비스를 받을 수 없도록 하는 방법이 사용된다.

도 1에는 일반적으로 DoS 공격이 이루어지는 서비스망이 도시되어 있다.

서비스거부 공격은 DoS 에이전트(Agent)가 심어진 컴퓨터(공격자)(11)에서 대량의 패킷을 발생시켜 호스트 컴퓨터(12)를 공격함으로써, 호스트 컴퓨터(12)가 정당한 다른 사용자들에게 서비스를 제대로 제공하지 못하도록 하는 행위를 말한다.

본 명세서에서는 DoS 에이전트가 심어진 공격자 컴퓨터(11)를 인터넷(13)에 연결하는 장비를 가입자 접속단(14)이라고 하는데, 이는 개인 이용자들이나 서비스를 목적으로 하지 않는 서버를 인터넷(13)에 연결하는 장비이다. 또한, 공격대상인 호스트 컴퓨터(12)를 인터넷(13)에 연결하는 장비를 호스트 접속단(15)이라고 하는데, 이는 서비스 제공을 목적으로 하는 서버를 인터넷(13)에 연결하는 장비이다. 일반적으로 가입자 접속단(14)과 호스트 접속단(15)은 라우팅 기능을 하는 에지 라우터(Edge-Router)로서, 자신이 관할하는 IP 주소군에 대한 정보를 가지고 있으며, 그 종류로는 라우터(Router), NAS(Network Access System), RAS(Remote Access System) 등이 있다.

일반적으로 서비스거부 공격은 공격자 컴퓨터(11)가 IP 주소를 위장하면서 공격 목표 호스트 컴퓨터(12)에 TCP 접속을 위한 동기신호를 무한으로 되풀이하여 보냄으로써 이루어지는데, 호스트 컴퓨터(12)는 이 위장된 IP 주소에 접속을 위한 신호를 응답하여 접속준비가 되었음을 무한으로 되풀이하여 알리는 동작을 수행하기 때문에 호스트 컴퓨터에 과부하가 걸려서 정당 사용자에게 서비스를 제공할 수 없게 된다.

이러한 DoS 공격을 방지하기 위하여 종래에는 공격자의 가입자 접속단에서 출발지 주소를 분석하여 차단조치를 수행하는 방식과, 호스트 컴퓨터의 호스트 접속단에서 유입되는 트래픽에 대한 대역폭을 제한하여 차단조치를 수행하는 방식이 사용되었다.

공격자 컴퓨터는 DoS 공격을 위한 대량의 공격 패킷을 발생시키는데, 이 공격 패킷들은 랜덤한 출발지 주소와 동일한 목적지 주소를 갖는다. 이 공격 패킷들은 공격자 컴퓨터에서 가입자 접속단으로 전송된다.

이하에서는 도 2를 참조하여 공격자의 가입자 접속단이 패킷의 출발지 주소를 분석하여 차단조치를 수행하는 방식을 설명한다. 가입자 접속단은 DoS 공격을 차단하기 위하여, 이 공격 패킷들의 출발지 주소를 추출하고(S21), 패킷의 출발지 주소가 자신이 관할하는 IP 주소군에 속하는지를 판별하여(S22), 자신이 관할하는 IP 주소군에 속하는 패킷들은 목적지로 전송하고(S24), 자신이 관할하는 IP 주소군에 속하지 않은 패킷들은 폐기한다(S23).

이러한 DoS 공격 차단방법은, 공격자가 랜덤한 출발지 주소로 공격 패킷을 생성하는 DoS 공격을 차단하는데 효과가 있다. 그러나, 이 방법은 랜덤하게 형성된 출발지 주소가 모두 가입자 접속단의 관할 IP 주소군에 속해 있으면, DoS 공격 차단 효과는 없어지는 문제가 있다.

도 3에는 호스트 접속단이 호스트 컴퓨터로 유입되는 트래픽의 대역폭을 분석하여 DoS 공격을 차단하는 방법이 제시되어 있다.

호스트 접속단은 유입되는 패킷의 프로토콜을 분석하여 현재 사용 대역폭을 분석하고(S31), 해당 프로토콜에 할당된 대역폭과 현재의 사용 대역폭을 비교한다(S32). 호스트 접속단의 현재 사용 대역폭이 할당된 대역폭보다 작으면 해당 패킷을 목적지로 전송하고(S34), 현재 사용 대역폭이 할당된 대역폭보다 크면 해당 패킷을 폐기한다(S33).

이러한 DoS 공격 차단방법은, 해커가 DoS 공격을 하더라도 특정 프로토콜에 대한 대역폭이 제한되어 있으므로 DoS 공격을 차단할 수 있다. 그러나, 이러한 대역폭 제한을 이용한 DoS 공격 차단방법은, 망사업자 입장에서 보면 이미 공격 트래픽의 폭주로 인해 망 자원 소모 및 성능 저하와 같은 피해를 입은 상태이고, 호스트 입장에서도 정상적인 트래픽에 대한 접속도 막히게 되므로 실제적으로 DoS 공격에 대한 차단 효과가 상쇄되는 문제점이 있다.

상기에서 언급한 바와 같이 종래의 DoS 공격 차단방법은 부분적인 효과는 있으나, 근본적인 DoS 공격 차단은 하지 못하는 문제점이 있었다.

발명이 이루고자 하는 기술적 과제

상기와 같은 종래 기술의 문제점을 해결하기 위하여 본 발명은 공격자의 가입자 접속단에서 전송 패킷의 목적지 주소와 트래픽 볼륨을 분석하여 해당 패킷을 전송 또는 폐기함으로써, DoS 공격을 원천적으로 차단하는 시스템 및 방법을 제공하는 것을 목적으로 한다.

발명의 구성 및 작용

상기한 목적을 달성하기 위한 본 발명에 따른 가입자 컴퓨터와 인터넷을 연결하는 라우팅 기능을 구비한 가입자 접속단에서의 DoS 공격 차단시스템은,

상기 가입자 컴퓨터로부터 전송되는 패킷의 목적지 주소필드와 프로토콜 필드를 분석하여 상기 전송된 패킷을 목적지 주소 및 패킷의 종류별로 분류하는 패킷 분류수단과, 상기 각 목적지 주소 및 패킷의 종류별로 분류된 패킷의 트래픽 볼륨을 측정하는 트래픽 볼륨 측정수단과, 상기 측정된 트래픽 볼륨과 해당 목적지 주소 및 패킷의 종류에 따른 기준치 트래픽 볼륨을 비교하여 상기 측정된 트래픽 볼륨이 기준치 볼륨보다 크지 않으면 상기 패킷이 목적지 주소로 라우팅되도록 하는 트래픽 비교수단과, 상기 측정된 트래픽 볼륨이 기준치 볼륨보다 크면 상기 패킷을 폐기하는 패킷 폐기수단을 포함한 것을 특징으로 한다.

또한, 본 발명에 따른 가입자 컴퓨터와 인터넷을 연결하는 라우팅 기능을 구비한 가입자 접속단에서의 DoS 공격 차단방법은,

상기 가입자 컴퓨터로부터 전송되는 패킷의 목적지 주소필드와 프로토콜 필드를 분석하여 상기 전송된 패킷을 목적지 주소 및 패킷의 종류별로 분류하는 패킷 분류단계와, 상기 각 목적지 주소 및 패킷의 종류별로 분류된 패킷의 트래픽 볼륨을 측정하는 트래픽 볼륨 측정단계와, 상기 측정된 트래픽 볼륨과 해당 목적지 주소 및 패킷의 종류에 따른 기준치 트래픽 볼륨을 비교하여 상기 패킷을 전송 또는 폐기하는 패킷 처리단계를 포함한 것을 특징으로 한다.

또한, 본 발명에 따르면 가입자 접속단에 상술한 바와 같은 서비스거부 공격 차단방법을 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체가 제공된다.

이하, 첨부된 도면을 참조하면서 본 발명의 한 실시예에 따른 "서비스거부 공격 차단시스템 및 방법"을 보다 상세하게 설명하기로 한다.

앞서 설명하였듯이, DoS 에이전트가 심어진 공격자 컴퓨터는 DoS 공격을 위한 대량의 공격 패킷을 발생시키는데, 이 공격 패킷들은 랜덤한 출발지 주소와 동일한 목적지 주소를 갖는다. 이 공격 패킷들은 공격자 컴퓨터에서 가입자 접속단에 전송된다. DoS 공격시 동일 목적지로 패킷이 집중되기 때문에 이 목적지에 대한 트래픽 볼륨이 급격하게 증가하게 된다. 본 발명은 이러한 DoS 공격의 특성을 이용해 동일 목적지를 가지는 패킷의 트래픽 볼륨이 일정 기준치 이상으로 증가하면 해당 패킷을 폐기하는 방법을 사용한다.

도 4는 본 발명에 따른 가입자 접속단에서의 목적지주소 분석을 통한 서비스거부 공격 차단시스템을 도시한 블록도이다.

가입자 접속단은 공격자 컴퓨터로부터 전송되는 IP 패킷을 분석하여 목적지 주소로 라우팅하는 기능을 수행하는데, 이 가입자 접속단에 IP 패킷을 분석하여 DoS 공격을 차단하는 시스템이 설치된다.

도 4를 참조하면, DoS 공격 차단시스템은 패킷 분류수단(41), 트래픽 볼륨 측정수단(42), 트래픽 볼륨 비교수단(43), 패킷 라우팅수단(44), 패킷 폐기수단(45), 및 이벤트 발생수단(46)을 포함한다.

패킷 분류수단(41)은 공격자 컴퓨터로부터 전송된 IP 패킷의 목적지 주소 필드와 프로토콜 필드를 분석하여 목적지 주소 및 패킷의 종류별로 해당 패킷을 분류하여 분류된 패킷을 트래픽 볼륨 측정수단(42)에 전달한다. IP 패킷의 종류로는 ICMP, TCP, UDP 등이 있으며, IP 패킷이 유입되면 목적지 주소와 패킷의 종류를 고려하여 패킷을 분류한다. 즉, 1번 목적지의 ICMP 패킷, 5번 목적지의 UDP 등과 같이 분류하여 트래픽 볼륨 측정수단(42)에 전달한다.

트래픽 볼륨 측정수단(42)은 이 패킷 분류수단(41)에서 목적지 주소 및 패킷의 종류별로 분류된 각각의 패킷의 트래픽 볼륨을 측정하여 트래픽 볼륨 비교수단(43)에 전달한다. 즉, 트래픽 볼륨 측정수단은 해당 목적지의 IP 패킷의 카운트를 하나 증가시킴으로써, 트래픽 볼륨을 측정한다. 즉, 패킷 분류수단(41)에서 분류된 IP 패킷이 1번 목적지의 ICMP 이면, 트래픽 볼륨 측정수단(42)은 (1, ICMP) 항목을 1 증가시키고, 다음 패킷 분류수단(41)에서 분류된 IP 패킷이 2번 목적지의 UDP 이면 트래픽 볼륨 측정수단(42)은 (2, UDP) 항목을 1 증가시킴으로써 트래픽 볼륨을 증폭한다.

트래픽 볼륨 비교수단(43)은 트래픽 볼륨 측정수단(42)에서 측정된 트래픽 볼륨과 기준 트래픽 볼륨을 비교하는데, 이 기준 트래픽 볼륨은 동일 목적지로 전송될 수 있는 특정한 종류의 패킷의 최대 트래픽 볼륨을 의미한다. 이 기준 트래픽 볼륨은 트래픽 엔지니어링, 즉 가입자의 트래픽을 직접 측정해서 통계치를 이용하여 얻어지는데, 하나의 목적지로 전송되는 특정 패킷의 볼륨은 통계치 범위내에 있으며 그 값 중 평균치를 뽑아서 기준 트래픽 볼륨으로 취한다. 또한, 이 기준 트래픽 볼륨은 망 사업자 정책이나 가입자 특성에 따라 달라질 수 있다.

패킷 라우팅수단(44)은 트래픽 볼륨 비교수단(43)의 비교결과, 현재 측정된 패킷의 트래픽 볼륨이 기준 트래픽 볼륨보다 작으면 해당 IP 패킷을 목적지 주소로 라우팅한다.

한편, 트래픽 볼륨 비교수단(43)의 비교결과 현재 측정된 패킷의 트래픽 볼륨이 기준 트래픽 볼륨을 초과하면, 패킷 폐기수단(45)은 해당 IP 패킷을 폐기하고, 이벤트 발생수단(46)은 알람이나 이벤트를 발생한다. 또한, 본 발명은 패킷 폐기수단이 아닌 원격 패킷 폐기수단(미도시)을 포함할 수 있는데, 이 원격 패킷 폐기수단은 원격지에서 이벤트 발생수단(46)에서 발생된 알람이나 이벤트를 분석하여 해당 IP 패킷을 차단하는 기능을 수행한다.

도 5는 이러한 목적지 주소 분석을 통한 DoS 공격 차단방법을 도시한 동작 흐름도이다.

가입자 접속단은 가입자 컴퓨터로부터 전송되는 패킷의 목적지 주소 필드와 프로토콜 필드를 분석하여 해당 패킷의 종류를 얻어내고(S51), 동일한 목적지 주소로 향하는 특정 종류의 패킷의 트래픽 볼륨을 측정한다(S52). 즉, IP 패킷을 목적지 주소와 패킷의 종류를 고려하여 분류하고, 이 분류된 목적지 주소와 패킷의 종류에 해당하는 카운터를 카운팅하여 패킷의 트래픽 볼륨을 측정한다.

이 동일한 목적지-주소로 향하는 특정 종류 패킷의 트래픽 볼륨을 기준치 트래픽 볼륨과 비교하여(S53), 현재 측정한 트래픽 볼륨이 기준치 트래픽 볼륨보다 적으면 해당 패킷을 목적지로 전송하고(S55), 현재 측정한 트래픽 볼륨이 기준치 트래픽 볼륨보다 크면 해당 패킷을 폐기하고 알람 또는 이벤트를 발생한다(S54). 여기서, 가입자 접속단은 알람 또는 이벤트를 발생하고 해당 패킷은 원격지에게 폐기할 수도 있다.

이러한 본원발명에 따르면 해커가 DoS 공격을 하더라도 가입자 접속단에서 목적지 주소에 대한 트래픽 볼륨을 분석하여 차단조치를 취함으로써, DoS 공격을 원천적으로 차단할 수 있다. 이러한 방식은, 망사업자 입장에서 보면 공격 트래픽을 출발지에서 차단하기 때문에 폭주로 인한 망 자원 및 성능저하 같은 피해를 막을 수 있고, 공격 대상 호스트 입장에서도 집중적인 트래픽 공격을 출발지에서 차단해주기 때문에 실제적으로 DoS 공격을 피할 수 있게 된다.

위에서 양호한 실시예에 근거하여 이 발명을 설명하였지만, 이러한 실시예는 이 발명을 제한하려는 것이 아니라 예시하려는 것이다. 이 발명이 속하는 분야의 숙련자에게는 이 발명의 기술사상을 벗어남이 없이 위 실시예에 대한 다양한 변화나 변경 또는 조절이 가능함이 자명할 것이다. 그러므로, 이 발명의 보호범위는 첨부된 청구범위에 의해서만 한정될 것이며, 위와 같은 변화예나 변경예 또는 조절예를 모두 포함하는 것으로 해석되어야 할 것이다.

발명의 효과

이상과 같이 본 발명에 의하면, 목적지주소를 대한 트래픽 볼륨의 분석을 통한 DoS 공격에 대한 효율적인 대응 방안을 제시한다. 이러한 본원 발명에 따른 방법을 가입자 접속단에 도입하면 DoS 공격을 근원적으로 효율적으로 차단할 수 있다. 즉, 망사업자 입장에서 보면 공격 트래픽을 출발지에서 차단함으로써 폭주로 인한 망 자원 고갈 및 성능저하 같은 피해를 막을 수 있고, 호스트 입장에서도 집중적인 트래픽 공격을 출발지에서 차단해 줌으로써 실제적으로 DoS 공격을 피할 수 있게 되는 효과가 있다.

(57) 청구의 범위

청구항 1.
가입자 컴퓨터와 인터넷을 연결하는 가입자 접속단의 IP 패킷을 분석하여 서비스거부(DoS) 공격을 차단하는 시스템에 있어서,

가입자 컴퓨터로부터 전송되는 패킷의 목적지 주소필드와 프로토콜 필드를 분석하여 상기 전송된 패킷을 목적지 주소 및 패킷의 종류별로 분류하는 패킷 분류수단;

상기 각 목적지 주소 및 패킷의 종류별로 분류된 패킷의 트래픽 볼륨을 측정하는 트래픽 볼륨 측정수단;

상기 측정된 트래픽 볼륨과 해당 목적지 주소 및 패킷의 종류에 따른 기준치 트래픽 볼륨을 비교하여 상기 측정된 트래픽 볼륨이 기준치 볼륨보다 크지 않으면 상기 패킷이 목적지 주소로 라우팅되도록 하는 트래픽 비교수단; 및

상기 측정된 트래픽 볼륨이 기준치 볼륨보다 크면 상기 패킷을 폐기하는 패킷 폐기수단을 포함 하는 서비스거부 공격 차단시스템.

청구항 2.
제 1 항에 있어서,

상기 특정된 트래픽 볼륨이 기준치 볼륨보다 크면 알람이나 이벤트를 발생하는 이벤트 발생수단을 더 포함하는 서비스거부 공격 차단시스템.

청구항 3.
제 2 항에 있어서,

상기 이벤트 발생수단에서 발생된 알람이나 이벤트를 분석하여 원격에서 해당 패킷을 차단하는 원격 패킷 폐기수단을 더 포함하는 서비스거부 공격 차단시스템.

청구항 4.
가입자 컴퓨터와 인터넷을 연결하는 가입자 접속단의 IP 패킷을 분석하여 서비스거부(DoS) 공격을 차단하는 방법에 있어서,

가입자 컴퓨터로부터 전송되는 패킷의 목적지 주소필드와 프로토콜 필드를 분석하여 상기 전송된 패킷을 목적지 주소 및 패킷의 종류별로 분류하는 단계;

상기 각 목적지 주소 및 패킷의 종류별로 분류된 패킷의 트래픽 볼륨을 측정하는 단계;

상기 측정된 트래픽 볼륨과 해당 목적지 주소 및 패킷의 종류에 따른 기준치 트래픽 볼륨을 비교하는 단계; 및

상기 기준치와의 비교결과에 따라 상기 패킷을 목적지로 전송하거나 폐기하는 단계를 포함하는 서비스거부 공격 차단방법.

청구항 5.
제 4 항에 있어서,

상기 측정된 트래픽 볼륨이 기준치 볼륨보다 크지 않으면 상기 패킷이 목적지 주소로 라우팅되도록 하고, 상기 측정된 트래픽 볼륨이 기준치 볼륨보다 크면 상기 패킷을 폐기하는 서비스거부 공격 차단방법.

청구항 6.
제 4 항에 있어서,

상기 특정된 트래픽 볼륨이 기준치 볼륨보다 크면 알람이나 이벤트를 발생시키는 단계를 포함하는 서비스거부 공격 차단방법.

청구항 7.
제 6 항에 있어서,

상기 이벤트 발생단계에서 발생된 알람이나 이벤트를 분석하여 원격지에서 해당 패킷을 차단하는 단계를 더 포함하는 서비스거부 공격 차단방법.

청구항 8.
가입자 컴퓨터와 인터넷을 연결하는 가입자 접속단에서,

상기 가입자 컴퓨터로부터 전송되는 패킷의 목적지 주소필드와 프로토콜 필드를 분석하여 상기 전송된 패킷을 목적지 주소 및 패킷의 종류별로 분류하는 단계;

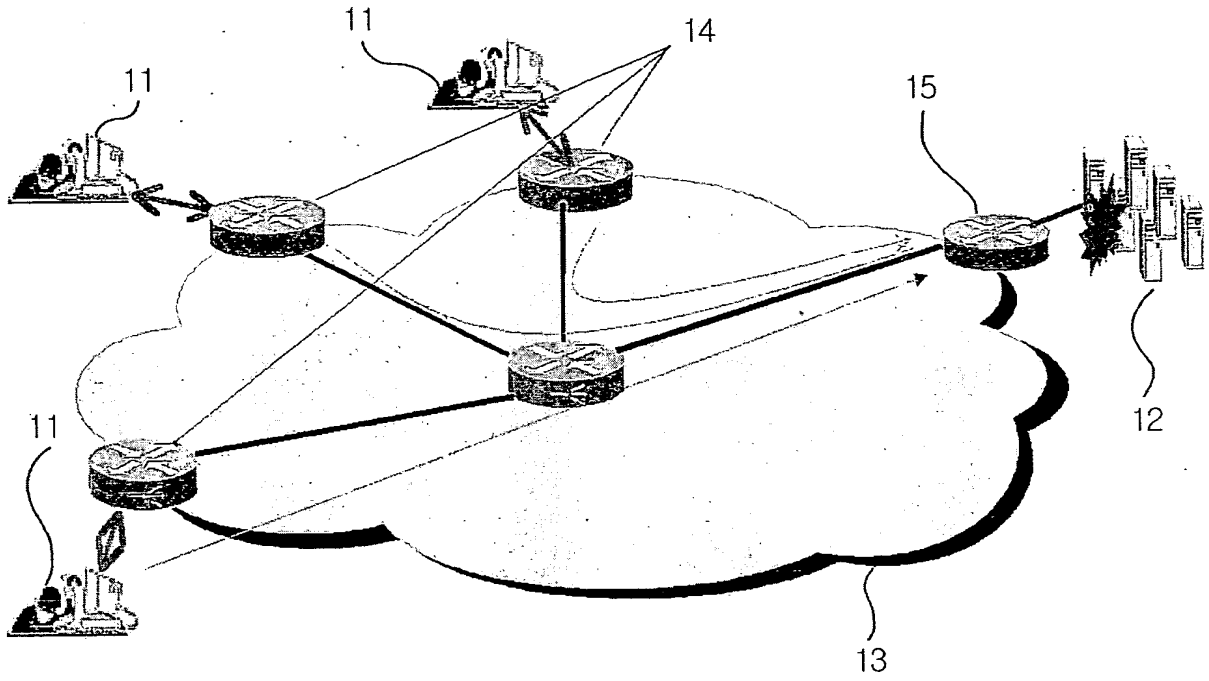
상기 각 목적지 주소 및 패킷의 종류별로 분류된 패킷의 트래픽 볼륨을 측정하는 단계;

상기 측정된 트래픽 볼륨과 해당 목적지 주소 및 패킷의 종류에 따른 기준치 트래픽 볼륨을 비교하는 단계; 및

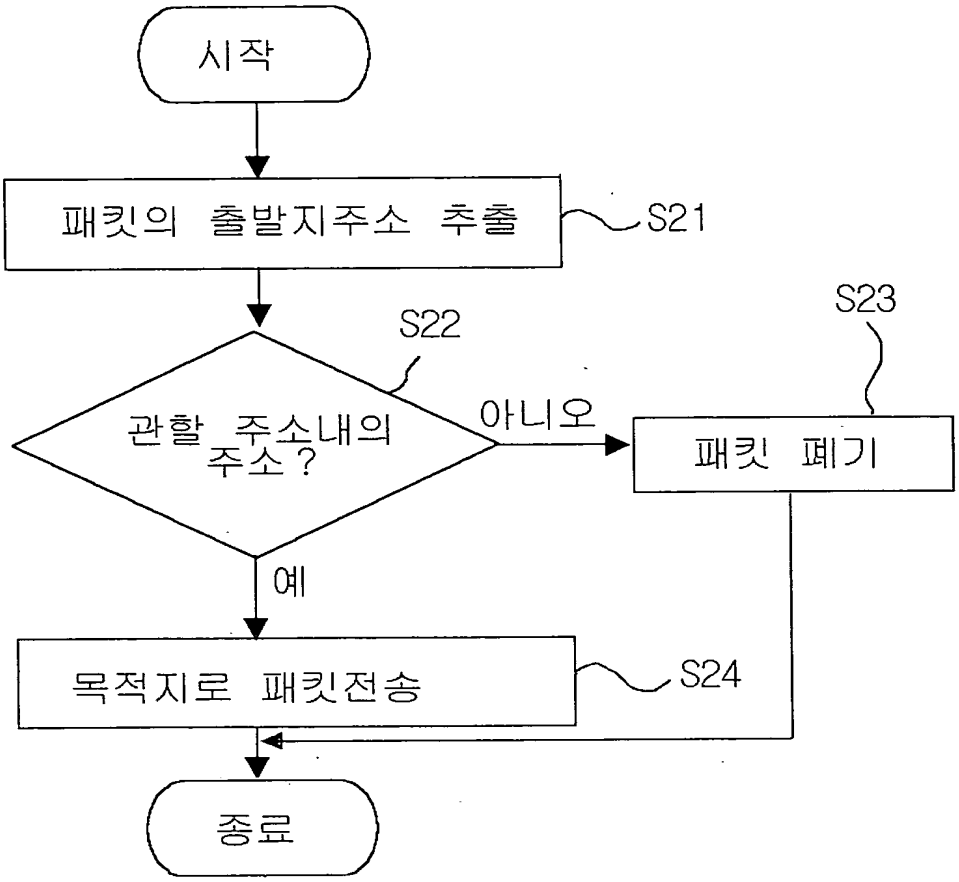
상기 측정된 트래픽 볼륨이 기준치 볼륨보다 크지 않으면 상기 패킷이 목적지 주소로 라우팅되도록 하고, 상기 측정된 트래픽 볼륨이 기준치 볼륨보다 크면 상기 패킷을 폐기하는 단계를 실행시키는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

도면

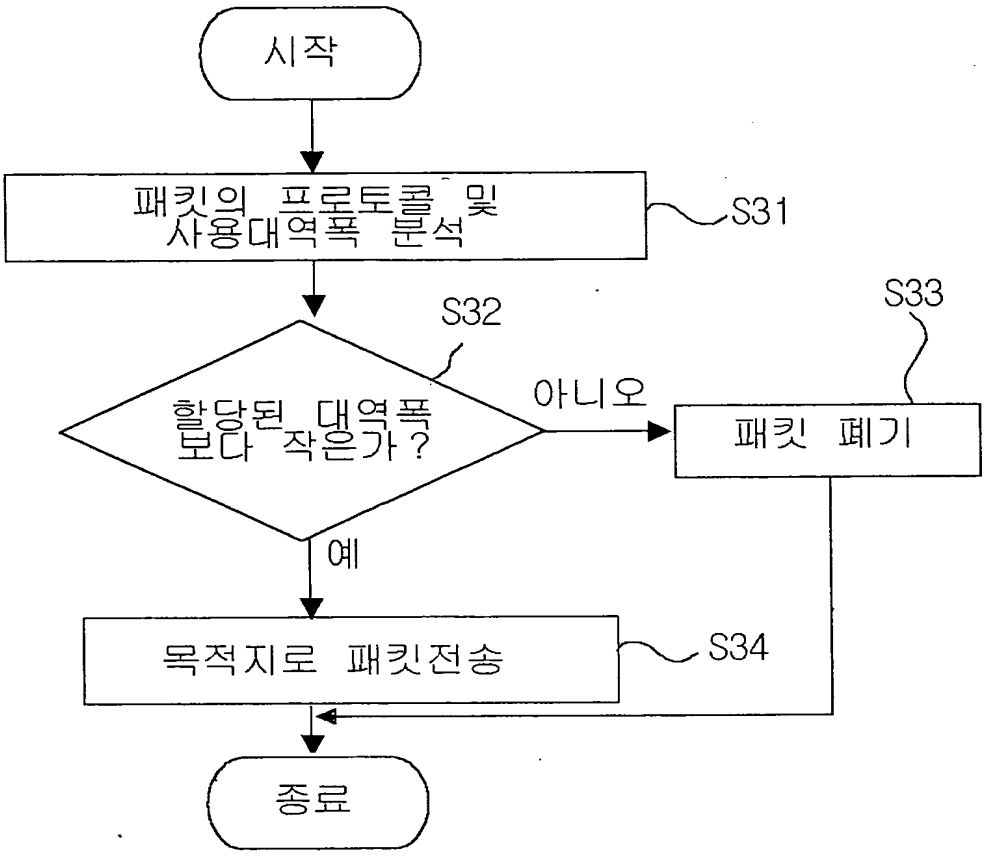
도면 1



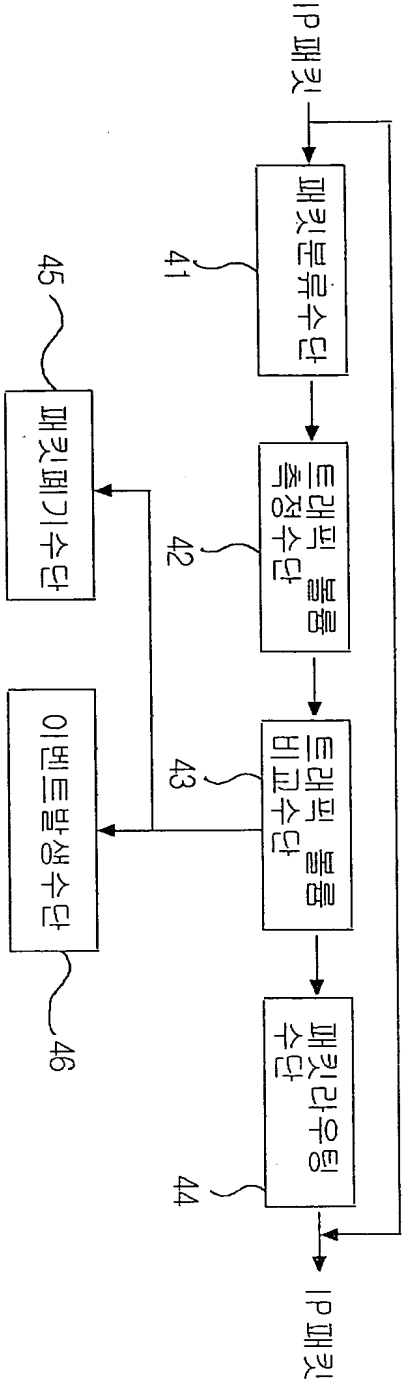
도면 2


시작
패킷의 출발지주소 추출
S21
S22
관할 주소내의 주소?
아니오
S23
패킷 폐기
예
목적지로 패킷전송
S24
종료

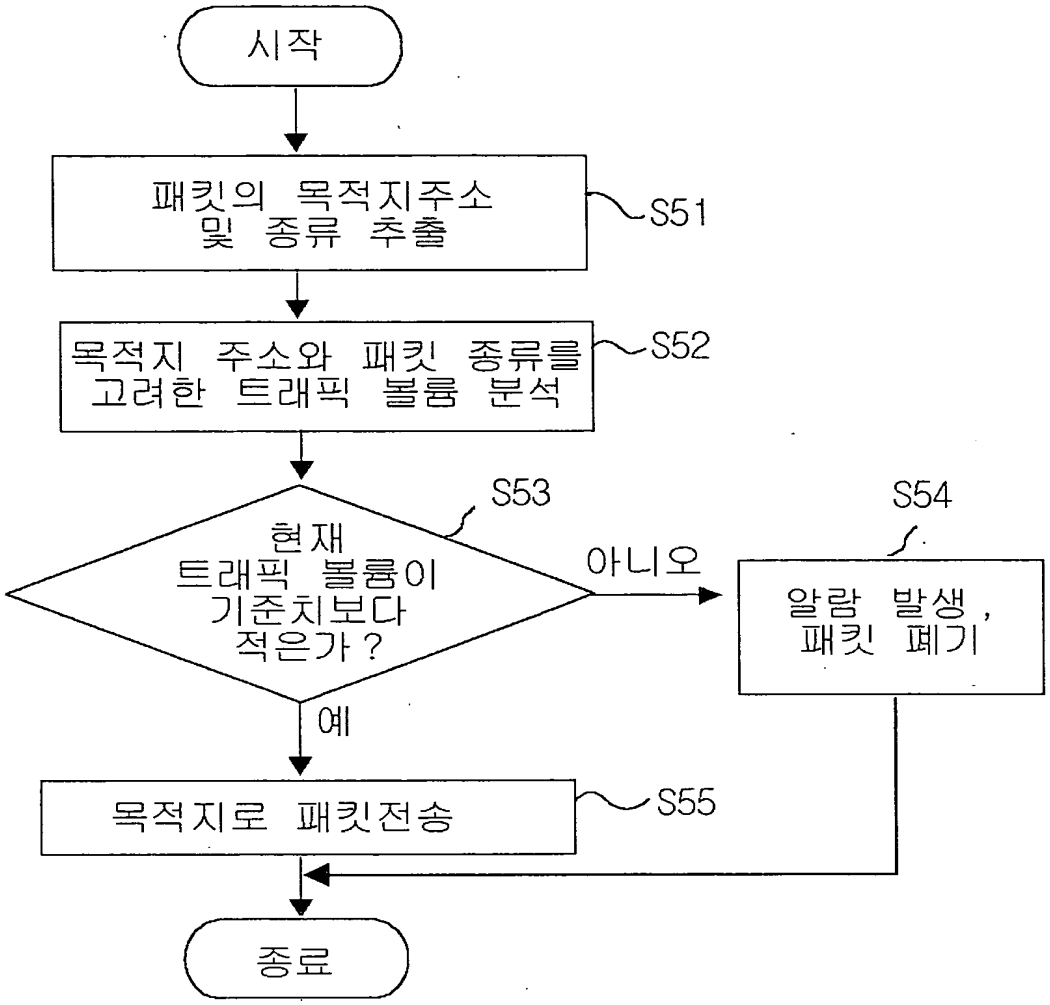
도면 3


시작
패킷의 프로토콜 및 사용대역폭 분석
S31
S32
할당된 대역폭 보다 작은가?
아니오
S33
패킷 폐기
예
목적지로 패킷전송
S34
종료

도면 4


IP 패킷
패킷분류수단
41
트래픽 볼륨 측정수단
42
트래픽 볼륨 비교수단
43
패킷라우팅 수단
44
IP 패킷
패킷폐기수단
45
이벤트발생수단
46

도면 5


시작
패킷의 목적지주소 및 종류 추출
S51
목적지 주소와 패킷 종류를 고려한 트래픽 볼륨 분석
S52
현재 트래픽 볼륨이 기준치보다 적은가?
S53
아니오
S54
알람 발생, 패킷 폐기
예
목적지로 패킷전송
S55
종료